

Approximating uniform quantum channels

Shmuel Friedland*

Dept. of Mathematics, Statistics and Computer Science,
Univ. of Illinois at Chicago,
Chicago, Illinois 60607-7045, USA
friedlan@uic.edu

March 26, 2014

Abstract

Let \mathcal{G} be a finite subgroup of unitary matrices acting on the space of N -qubits. We associate with \mathcal{G} a uniform quantum channel QU from the space on N -qubits to itself. We give a quantum algorithm to approximate this channel by considering a set of generators on \mathcal{G} . Under suitable assumptions this approximation is BPQ. We then apply this approximation to study the orbit equivalence of two density matrices under the action of \mathcal{G} . We show that for some special cases of \mathcal{G} and two pure states the orbit equivalence in BPQ, if a specific quantum observation can be implemented efficiently. We discuss the application of our problem to the graph isomorphism problem.

2010 Mathematics Subject Classification: 03D15, 05C50, 05C60, 15A69, 65C40, 68Q12, 68R10, 94A40.

Keywords and phrases: Cayley graph, density matrices, fidelity, graph isomorphism problem, orbit equivalence, quantum algorithm, quantum channel, second eigenvalue of the Laplacian, uniform quantum channel.

1 Introduction

Let \mathcal{G} a finite group. Consider the space $\mathbb{C}^{\mathcal{G}}$ of all complex-valued vectors $\mathbf{v} = (v_g)_{g \in \mathcal{G}}$. Assume that $\mathbb{C}^{\mathcal{G}}$ is equipped with the inner product $\mathbf{u}^\dagger \mathbf{v}$. For each subset $T \subset \mathcal{G}$ we denote by $\mathbf{1}_T$ the characteristic vector of T . Let $\mathbf{1} := \mathbf{1}_{\mathcal{G}}$. Let $|g\rangle := \mathbf{1}_{\{g\}}$, $g \in \mathcal{G}$ be the standard basis in $\mathbb{C}^{\mathcal{G}}$. It is well known that for many classical groups one can generated efficiently the uniform quantum state [3, 20, 21]

$$\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g\rangle. \quad (1.1)$$

Let $\otimes^N \mathbb{C}^2$ be the Hilbert space of dimension 2^N corresponding to N -qubit system. Let $|x\rangle$ denote $|x_{N-1}\rangle \otimes \dots \otimes |x_0\rangle$ the untangled state of N qubits, where each qubit is in up or down positions. Here $x \in \{0, 1, \dots, 2^N - 1\}$ is an integer, written in the binary basis $x = x_{N-1} \dots x_0$, where $x_j \in \{0, 1\}$, $j = 0, \dots, N - 1$. So

*Supported by NSF grant DMS-1216393.

$|x\rangle, x = 0, \dots, 2^N - 1$ is the standard basis in $\otimes^N \mathbb{C}^2$. Assume that \mathcal{G} has representation as a finite group of unitary matrices acting on $\otimes^N \mathbb{C}^2$.

For a given untangled N -qubit $|x\rangle \in \otimes^N \mathbb{C}^2$ consider the following uniform quantum state on $\mathbb{C}^{\mathcal{G}} \otimes (\otimes^N \mathbb{C}^N)$:

$$\frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} |g\rangle \otimes g|x\rangle. \quad (1.2)$$

Assuming that the state (1.1) can be generated efficiently then the above state can be generated efficiently. Suppose we can generate efficiently the uniform quantum state corresponding to the orbit of x , denoted by $\text{orb}(|x\rangle) := \cup_{g \in \mathcal{G}} \{g|x\rangle\}$ under the action of \mathcal{G}

$$\frac{1}{\kappa(\mathcal{G})} \sum_{g \in \mathcal{G}} g|x\rangle. \quad (1.3)$$

(Here $\kappa(G)$ is a normalization constant.) Then we can solve efficiently the graph isomorphism problem (GIP) [1].

The aim of this paper is to study the efficient implementation of the mixed state, i.e., density matrix, which is an analog of the state (1.3):

$$\frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} g|x\rangle \langle x|g^\dagger. \quad (1.4)$$

Consider the symmetric group S_n of degree n . Let $N = \binom{n}{2}$ and consider the space of N -qubits $\otimes^N \mathbb{C}^2$. View each standard basis $|x\rangle, x = x_{(n-1)n} \dots x_{12}$ as a labeled graph $G(x)$ on n vertices $[n] := \{1, \dots, n\}$. So $x_{ij} \in \{0, 1\}$ represents the edge (i, j) , where $1 \leq i < j \leq n$. Thus $G(x)$ contains the edge (i, j) if and only if $x_{ij} = 1$. S_n acts as a subgroup of permutation $\pi : S_n \rightarrow S_N$ on the set of edges $[N]$. Let $P : S_n \rightarrow \mathcal{G}$ be the representation of S_n as a subgroup of permutation acting on $\otimes^N \mathbb{C}^2$ as follows. $P(\sigma)|x\rangle = |\pi(\sigma)(x)\rangle$ for $x = 0, \dots, 2^N - 1$. The main result of this paper that the mixed state (1.4) can be efficiently approximated for groups \mathcal{G} which are efficiently represented, see §2. In particular, S_n is efficiently represented.

However, this approximation result does not imply that the GIP can be solved efficiently. Our approximation result will imply that the GIP will be solved efficiently if we assume the hypothesis:

Hypothesis 1 *Let ρ be a diagonal density matrix on the N -th qubit state:*

$$\rho = \sum_{x=1}^{2^N-1} \lambda_x |x\rangle \langle x|, \quad \lambda_x \geq 0, x = 0, \dots, 2^N - 1, \quad \sum_{x=0}^{2^N-1} \lambda_x = 1. \quad (1.5)$$

Then for each $y \in \{0, \dots, 2^N - 1\}$ the eigenvalue $\lambda_y = \langle y|\rho|y\rangle$ can be measured efficiently.

The above hypothesis is in line with postulates of quantum mechanics [18, Postulate 3, §2.2.3]. Namely, if $|\psi\rangle$ is an eigenstate of an observable A then upon measuring $|\psi\rangle$ one observes with probability one the eigenvalue $\langle \psi|A|\psi\rangle$ [18, (2.103), §2.2.5]. However, we do not know how measure λ_y efficiently. The standard approach to measure λ_y is given in [5, 17]. Namely, $\lambda_y = \text{tr}(\rho(|y\rangle\langle y|))$. As it will be explained in §4 this measurement can not be implemented efficiently in this case.

We now give a brief survey of the rest of the paper. In §2 we discuss the uniform quantum channel QU , which maps the mixed states on N -qubit space to itself:

$$QU(\rho) = \sum_{g \in \mathcal{G}} \frac{1}{|\mathcal{G}|} g \rho g^\dagger. \quad (1.6)$$

We define a quantum channel Q_N acting on the space of N -qubits in terms of generators of \mathcal{G} . We give a standard way to generate Q_N by adding the environment qubit space. We show that QU can be efficiently approximated by l -th power of Q_N for efficiently represented groups \mathcal{G} . In §3 we discuss briefly the known techniques for estimation of $\text{tr } \rho \eta$ for two mixed states ρ, η . In §4 discuss the application of our results to the GIP.

2 Uniform quantum channels

Denote by $\Delta(N) \subset \mathbb{H}_{2^N}$ the set of density matrices of Hermitian matrices of order 2^N . Recall that $Q : \Delta(N) \rightarrow \Delta(N)$ is called a quantum channel [18] if

$$Q(\rho) = \sum_{i=1}^k A_i \rho A_i^\dagger, \quad A_i \in \mathbb{C}^{2^N \times 2^N}, \quad \sum_{i=1}^k A_i^\dagger A_i = I. \quad (2.1)$$

Here k is any positive integer, and $\mathbb{C}^{m \times n}$ denotes the space of $m \times n$ complex valued matrices. It is straightforward to show that a product of two quantum channels, (as operators) is a quantum channel.

Assume that $\mathbf{u} = (u_g)_{g \in \mathcal{G}}$ is a probability vector on \mathcal{G} , i.e. each $u_g \geq 0$ and $\sum_{g \in \mathcal{G}} u_g = 1$. We associate with \mathbf{u} the following quantum channel

$$Q(\mathbf{u})(\rho) = \sum_{g \in \mathcal{G}} u_g g \rho g^\dagger, \quad \rho \in \Delta(N). \quad (2.2)$$

Recall that $\frac{1}{|\mathcal{G}|} \mathbf{1}$ the uniform distribution on \mathcal{G} . Then QU given by (1.6) is equal to $Q(\frac{1}{|\mathcal{G}|} \mathbf{1})$. Let $S \subset \mathcal{G}$ be a symmetric generating subset of \mathcal{G} . So $g \in S \iff g^{-1} \in S$ and S generates \mathcal{G} . (We assume $id \notin S$.) S induces the Cayley graph denoted as $\Gamma(\mathcal{G}, S)$ [14]. The vertices of this graph are the elements of \mathcal{G} . A vertex $g \in \mathcal{G}$ is connected to all vertices of the form hg for $h \in S$. $\Gamma(\mathcal{G}, S)$ is undirected and $|S|$ -regular. Let $A(\mathcal{G}, S)$ be the adjacency matrix of this graph. The Laplacian $L(\mathcal{G}, S)$ is given by $|S|I - A(\mathcal{G}, S)$. Since $\Gamma(\mathcal{G}, S)$ is connected and $|S|$ -regular, the eigenvalues of $L(\mathcal{G}, S)$ satisfy the inequalities

$$\lambda_1 = 0 < \lambda_2 \leq \dots \leq \lambda_{|\mathcal{G}|} \leq 2|S|. \quad (2.3)$$

Denote

$$M(\mathcal{G}, S) := \frac{1}{1 + |S|} (I + A(\mathcal{G}, S)). \quad (2.4)$$

Then the above matrix is symmetric, irreducible and doubly stochastic. So its eigenvalues are $\mu_j = \frac{|S|+1-\lambda_j}{|S|+1}$ for $j = 1, \dots, |\mathcal{G}|$. Note that the uniform vector $\frac{1}{|\mathcal{G}|} \mathbf{1}$ is the eigenvector corresponding to $\mu_1 = 1$. All other eigenvalues μ of satisfy the inequality

$$|\mu| \leq \max(1 - \frac{\lambda_1}{|S|+1}, 1 - \frac{2}{|S|+1}). \quad (2.5)$$

Definition 2 \mathcal{G} is called efficiently represented on N -qubit system if the following conditions hold:

1. The order of $\log |\mathcal{G}|$ is polynomial in N :

$$\log |\mathcal{G}| \leq bN^\beta, \quad 0 < b, \beta. \quad (2.6)$$

2. There exists a symmetric set of generators S such that the following conditions hold:

(a) Each $g \in S$ can be implemented by at most bN^β elementary quantum gates.

(b)

$$|S| \leq bN^\beta, \quad (2.7)$$

$$\lambda_1(L(\mathcal{G}, S))^{-1} \leq bN^\beta. \quad (2.8)$$

In §4 we show that the representation of S_n on the $N = \binom{n}{2}$ qubit space, as discussed in Introduction, is efficiently represented.

In what follows we assume that \mathcal{G} is efficiently represented on N -qubit system. Let

$$Q_N := Q\left(\frac{1}{1+|S|} \mathbf{1}_{\{id\} \cup S}\right). \quad (2.9)$$

Our first major result is that Q_N can be implemented efficiently. That is, given a density matrix $\rho \in \Delta(N)$, we can obtain $Q_N(\rho)$ using $O(N^{2\beta})$ elementary quantum gates. This implementation of $Q_N(\rho)$ is obtained by use of $\lceil \log_2 N \rceil$ ancillary qubits, which are treated as the *environment* qubits [18].

A standard way to construct a quantum channel acting on $d \times d$ density matrices ρ is as follows [18]. Introduce a fixed environment density matrix ρ_{env} , (acting on the environment space \mathbb{C}^e), and consider the joint product density matrix $\rho_{tot} := \rho_{env} \otimes \rho$ acting on $\mathbb{C}^e \otimes \mathbb{C}^d$. Apply a unitary gate U on ρ_{tot} to obtain $U\rho_{tot}U^\dagger$. Next discard the environment, which is equivalent to “tracing out” the environment. (Equivalently, we never measure the environment or apply a unitary transformation on the environment.) This procedure gives rise to a new $d \times d$ density matrix $\mathcal{E}(\rho)$, where \mathcal{E} is a corresponding quantum channel which depends on ρ_{env} and U .

Assume first that $|S| = 2^m - 1$. Then our environment would be the following density matrix corresponding to the uniform pure state on m qubits:

$$\rho_{env} := \left(\otimes^m \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \left(\otimes^m \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) \right). \quad (2.10)$$

Our U is a product of the following $2^m - 1$ controlled gates, with respect to the m -environment qubits. Assume that the standard basis of m -qubits is given by $|a\rangle = |a_{m-1} \dots a_0\rangle$, where $a = a_{m-1}2^{m-1} + \dots + a_0$. Let $S = \{g_1, \dots, g_{2^m-1}\}$. For $a > 0$ the controlled gate $V_a := U_{C_{g_a}}$ acts as follows.

$$V_a(|b\rangle \otimes |\psi\rangle) = |b\rangle \otimes |\psi\rangle, \text{ for } b \neq a, \quad V_a(|a\rangle \otimes |\psi\rangle) = |a\rangle \otimes g_a|\psi\rangle.$$

Recall that to implement V_a we need to use $\Theta(m^2)$ CNOT gates plus the number of gates needed to perform g_a [18]. Hence we need $O(N^\beta + (\log N)^2) = O(N^\beta)$ gates.

U is obtained by applying V_1, \dots, V_{2^m-1} in any order, since V_a are commuting. Thus we need $O(N^{2\beta})$ gates to implement U .

Observe next that U is the following block diagonal matrix of order $2^m \cdot 2^N$:

$$U = \text{diag}(g_0, g_1, \dots, g_{2^m-1}), \quad g_0 := id.$$

Write down $\rho_{env} \otimes \rho$ as the Kronecker product. In terms of a $2^m \times 2^m$ block matrix it is of the form $[\rho_{ij}]_{i,j=1}^{2^m}$, where $\rho_{ij} = 2^{-m} \rho$. Then

$$\begin{aligned} U(\rho_{env} \otimes \rho)U^\dagger &= [2^{-m} g_{i-1} \rho g_{i-1}^\dagger]_{i,j=1}^{2^m}, \\ Q_N(\rho) &= \text{tr}_{env} U(\rho_{env} \otimes \rho)U^\dagger. \end{aligned} \quad (2.11)$$

Thus we can construct the quantum channel Q_N in $O(N^{2\beta})$ operations if $|S| = 2^m - 1$.

We now discuss briefly the case where $2^{m-1} < |S| + 1 < 2^m$. We then consider the controlled V_a gates as above for $a = 1, \dots, |S|$. So $U = V_1 \dots V_{|S|}$. We now assume that

$$\rho_{env} = |\phi\rangle\langle\phi|, \quad \phi = \frac{1}{\sqrt{|S|+1}} \sum_{0 \leq a \leq |S|} |a\rangle.$$

Then (2.11) holds. Again we need $O(N^{2\beta})$ operations to construct the quantum channel Q_N .

For a hermitian matrix A define the nuclear norm $\|A\|_1$ as the sum of the absolute values of the eigenvalues of A . Our next observation is that the uniform quantum channel QU can be efficiently approximated by a suitable l power of Q_N . That is, one has the inequality:

$$\|QU(\rho) - Q_N^l(\rho)\|_1 \leq e^{\frac{bN^\beta}{2} - \frac{l}{(bN^\beta+1)^2}} \quad (2.12)$$

Denote by $\Pi(\mathcal{G})$ the set of probability vectors on \mathcal{G} . For $\mathbf{v} \in \mathbb{C}^m$ denote by $\|\mathbf{v}\|$ and $\|\mathbf{v}\|_1$ the Euclidean norm and the ℓ_1 norm of \mathbf{v} respectively.

Lemma 3 *Let \mathcal{G} be a finite group of unitary matrices acting on $\otimes^N \mathbb{C}^2$. Assume that \mathcal{G} satisfies the assumptions of Definition 2. Let $\mathbf{u} \in \Pi(\mathcal{G})$ and $l \in \mathbb{N}$. Then*

$$\left\| \frac{1}{|\mathcal{G}|} \mathbf{1} - M(\mathcal{G}, S)^l \mathbf{u} \right\| < \left(1 - \frac{1}{(bN^\beta + 1)^2} \right)^l < e^{-\frac{l}{(bN^\beta+1)^2}}. \quad (2.13)$$

Proof. Recall that 1 is an algebraically simple eigenvalue of $M(\mathcal{G}, S)$. Furthermore, each other eigenvalue $\mu \neq 1$ of $M(\mathcal{G}, S)$ satisfies the inequality (2.5). Since $|S| \geq 1$, the inequalities (2.7) and (2.8) yield that

$$|\mu| \leq 1 - \frac{1}{bN^\beta(|S|+1)} \leq 1 - \frac{1}{bN^\beta(bN^\beta+1)} \leq 1 - \frac{1}{(bN^\beta+1)^2}. \quad (2.14)$$

Observe next that $\|\mathbf{u}\| \leq 1$. Also $\mathbf{u} = \frac{1}{|\mathcal{G}|} \mathbf{1} + \mathbf{v}$, where $\mathbf{v}^\top \mathbf{1} = 0$. So $\|\mathbf{u}\|^2 = \frac{1}{|\mathcal{G}|} + \|\mathbf{v}\|^2$. Hence $\|\mathbf{v}\| < 1$. Clearly $\frac{1}{|\mathcal{G}|} \mathbf{1} - M(\mathcal{G}, S)^l \mathbf{u} = -M(\mathcal{G}, S)^l \mathbf{v}$. As the restriction of $M(\mathcal{G}, S)$ to all orthogonal vectors to $\mathbf{1}$ has at most the spectral norm $1 - \frac{1}{(bN^\beta+1)^2}$ we deduce the first part of the inequality (2.13). Clearly,

$$\frac{1}{t} \log(1-t) = \frac{1}{t} \left(- \sum_{j=1}^{\infty} \frac{t^j}{j} \right) = -1 - \left(\sum_{j=2}^{\infty} \frac{t^{j-1}}{j} \right) < -1, \quad \text{for } t \in (0, 1). \quad (2.15)$$

Set $t = (bN^\beta + 1)^{-2}$ and deduce the second part of the inequality (2.13). \square

Lemma 4 *Let $\mathbf{u} \in \Pi(\mathcal{G})$ and $Q(\mathbf{u})$ be the quantum channel given (2.2). Denote by Q_N the quantum channel $Q(\frac{1}{1+|S|}\mathbf{1}_{\{id\} \cup S})$:*

$$Q_N(\rho) := \sum_{g \in \{id\} \cup S} \frac{1}{1+|S|} g \rho g^\dagger. \quad (2.16)$$

Then $Q_N Q(\mathbf{u}) = Q(M(\mathcal{G}, S)\mathbf{u})$. In particular $Q_N^l = Q(M(\mathcal{G}, S)^l \mathbf{1}_{\{id\}})$. Furthermore for each density matrix $\rho \in \Delta(N)$ the inequality (2.12) hold.

Proof. Let $h \in \mathcal{G}$. Denote $B(h)$ the permutation on \mathcal{G} induced by h . So $B(h)(g) = hg$ for $g \in \mathcal{G}$. $B(h)$ acts on $\Pi(\mathcal{G})$ as follows. Let $\mathbf{u} = (u_g)_{g \in \mathcal{G}} \in \Pi(\mathcal{G})$. Then $B(h)\mathbf{u} = \mathbf{v} = (v_g)_{g \in \mathcal{G}}$, where $v_g = u_{hg}$. Denote by R the quantum channel $Q(\mathbf{1}_{\{h\}})$. A straightforward calculation shows that $RQ(\mathbf{u}) = Q(B(h)\mathbf{u})$. Use (2.16) to deduce the equalities $Q_N Q(\mathbf{u}) = Q(M(\mathcal{G}, S)\mathbf{u})$ and $Q_N^l = Q(M(\mathcal{G}, S)^l \mathbf{1}_{\{id\}})$.

Let $\mathbf{1}_{id} = \frac{1}{bN^\beta + 1} \mathbf{1} + \mathbf{v}$. Denote $\mathbf{v}_l = (v_{g,l})_{g \in \mathcal{G}} := M(\mathcal{G}, S)^l \mathbf{v}$. Lemma 3 yields that

$$\|\mathbf{v}_l\| < (1 - \frac{1}{(bN^\beta + 1)^2})^l < e^{-\frac{l}{(bN^\beta + 1)^2}}. \quad (2.17)$$

We now show (2.12). Let

$$A := QU(\rho) - Q_N^l(\rho) = - \sum_{g \in \mathcal{G}} v_{g,l} g \rho g^\dagger.$$

Assume that $A\mathbf{x}_j = \lambda_j \mathbf{x}_j$, $j = 1, \dots, 2^N$, where $\mathbf{x}_1, \dots, \mathbf{x}_{2^N}$ is an orthonormal basis in $\otimes^N \mathbb{C}^2$. Let $\mathbf{y}_j = \mathbf{x}_j$ if $\lambda_j \geq 0$ and $\mathbf{y}_j = -\mathbf{x}_j$ if $\lambda_j < 0$. Then

$$\|A\|_1 = \sum_{j=1}^{2^N} \mathbf{y}_j^\dagger A \mathbf{x}_j = - \sum_{g \in \mathcal{G}} v_{g,l} \sum_{j=1}^{2^N} \mathbf{y}_j^\dagger (g \rho g^\dagger) \mathbf{x}_j.$$

Clearly, $\|\eta\|_1 = 1$ for any density matrix $\eta \in \Delta(N)$. The maximal characterization of $\|\eta\|_1$ yields the inequality $|\sum_{j=1}^{2^N} \mathbf{y}_j^\dagger \eta \mathbf{x}_j| \leq \|\eta\|_1 = 1$ [11]. Hence

$$\|A\|_1 \leq \sum_{g \in \mathcal{G}} |v_{g,l}| \leq \sqrt{|\mathcal{G}|} \|\mathbf{v}_l\|_2.$$

Combine this inequality with (2.17) and (2.6) to deduce (2.12). \square

Let $\varepsilon > 0$ be given. Then

$$\|QU(\rho) - Q_N^l(\rho)\|_1 < \varepsilon, \quad \text{if } l = \frac{1}{2}(1 + \delta)bN^\beta(bN^\beta + 1)^2, \quad \delta = \frac{2}{bN^\beta} \log \frac{1}{\varepsilon}. \quad (2.18)$$

3 Orbit identification and fidelity

Let $\rho \in \Delta(N)$. Then $\text{orb}_{\mathcal{G}}(\rho) := \cup_{g \in \mathcal{G}} \{g\rho g^\dagger\}$ is the \mathcal{G} -orbit of ρ . Denote by $H(\rho)$ the stabilizer of ρ : $H(\rho) := \{g \in \mathcal{G}, g\rho g^\dagger = \rho\}$. The first problem is to determine $|H(\rho)|$, i.e., the cardinality of the stabilizer of ρ . The second problem is to determine if $\text{orb}_{\mathcal{G}}(\rho_1) = \text{orb}_{\mathcal{G}}(\rho_2)$ for two density matrices $\rho_1, \rho_2 \in \Delta(N)$.

Clearly, a necessary condition for $\text{orb}_{\mathcal{G}}(\rho_1) = \text{orb}_{\mathcal{G}}(\rho_2)$ is the condition

$$QU(\rho_1) = QU(\rho_2). \quad (3.1)$$

The problem of deciding when two density matrices are the same, in general, does not seem to have an efficient quantum algorithm. It is a special case of the problem: “How close are two given density matrices $\rho, \eta \in \Delta(N)$ ”? [18, §9.2]. Since we can only compute efficiently the density matrices $Q_N^l(\rho_1)$ and $Q_N^l(\rho_2)$, we indeed need to estimate how close these two approximate density matrices are. One way to find out is to compute the *fidelity* $F(\rho, \eta)$ [18]. Recall that $F(\rho, \eta) \leq 1$, and equality holds if and only if $\rho = \eta$. There are ways to estimate $F(\rho, \eta)$ but they are not efficient [17].

A basic algorithm for computing $F(\rho, \eta)$ is to evaluate $\text{tr } \rho\eta$ [5]. This is done by applying the controlled SWAP gate to $\rho \otimes \eta$ with an additional control qubit.

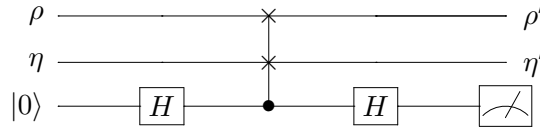


Figure 1: Quantum circuit based on controlled SWAP gate used to measure $\text{tr } \rho\eta$ between two mixed states ρ and η .

The reading of $|0\rangle$ is with probability $\frac{1}{2}(1 + \text{tr } \rho\eta)$. Suppose that $\eta = |\psi\rangle\langle\psi|$ is a pure state. Then $\text{tr } \rho\eta = \langle\psi|\rho|\psi\rangle$. Suppose furthermore that we assume as in Hypothesis 1 that ρ is of the form (1.5) and $|\psi\rangle = |y\rangle$. Then the probability to read $|0\rangle$ is $\frac{1}{2}(1 + \lambda_y)$.

Suppose that $\lambda_y > 0$. If λ_y^{-1} has a polynomial growth in N then we could estimate the value of λ_y in polynomial time with arbitrary precision. But if λ_y^{-1} has an exponential growth in N then we can not estimate the value of λ_y in polynomial time. We will show that this is the case for the graph isomorphism problem.

4 The graph isomorphism problem

Let K_n be the complete graph on n vertices. We identify the set of vertices and edges of K_n with $[n]$ and $\mathcal{E}_n := \{(1,2), \dots, (n-1,n)\}$ respectively. Let $G_1 = ([n], E_1), G_2 = ([n], E_2)$ be two simple undirected graphs $E_1, E_2 \subset \mathcal{E}_n$. G_1 and G_2 are called *isomorphic* if there exists a bijection $\sigma : [n] \rightarrow [n]$ which induces the corresponding bijection $\tilde{\sigma} : E_1 \rightarrow E_2$.

The graph isomorphism problem, is the computational complexity of determination if G_1 and G_2 are isomorphic. Clearly the *GIP* in the class *NP*. It is one of

a very small number of problems whose complexity is unknown [9, 13]. For certain graphs it was known that the complexity of *GIP* is polynomial [2, 4, 7, 15, 16].

The current approach for the *GIP* using quantum algorithms is to use the hidden subgroup problem [6, 12, 10, 19]. However, it was not very successful.

Recall the encoding of all labeled graphs on $[n]$ by $G(x), x \in \{0, \dots, 2^N - 1\}$, $N = \binom{n}{2}$ given in Introduction. Each nonzero integer $x = x_{(n-1)n} \dots x_{12}$ written in the binary form, $(0 \leq x \leq 2^{\binom{n}{2}} - 1)$. It will be convenient to denote $|x\rangle := \otimes_{1 \leq i < j \leq n} |e_{i,j,x_{ij}}\rangle$.

Let $\sigma \in S_n$. Then σ acts on $G(x)$ by renaming the edges according to the map $\sigma : [n] \rightarrow [n]$. So $\sigma(G(x)) = G(\pi(\sigma)(x))$. Denote by $\text{orb}(x) := \cup_{\sigma \in S_n} \{\pi(\sigma)(x)\}$ the orbit of x under the action of S_n .

Assume that σ is a transposition $\tau_{i,j}$, which interchanges i with j . Then the action of $\tau_{i,j}$ on any $G(x)$ is equivalent to $(n-2)$ transposition on the edges of $G(x)$. Hence the action of $\tau_{i,j}$ on $\otimes^N \mathbb{C}^2$ as achieved by $(n-2)$ swaps. We denote by $P(\sigma) \in U(2^N)$ the unitary matrix, which corresponds to the action of σ on the standard basis of $\otimes^N \mathbb{C}^2$. That is, $P(\sigma)|x\rangle = |\pi(\sigma)(x)\rangle$. Let $P : S_n \rightarrow \mathcal{G} \subset U(2^N)$ be the above representation of S_n . We will identify S_n with \mathcal{G} and no ambiguity will arise.

From the definition of the uniform quantum channel QU (1.6) we deduce

$$\rho(x) := QU(|x\rangle\langle x|) = \frac{1}{|S_n|} \sum_{\sigma \in S_n} |\pi(\sigma)(x)\rangle\langle \pi(\sigma)(x)| = \frac{|H(x)|}{|S_n|} \sum_{y \in \text{orb}(x)} |y\rangle\langle y|, \quad (4.1)$$

Here $H(x) \subset S_n$ and $\text{orb}(x)$ are the stabilizer of x , the automorphism group of $G(x)$, and the orbit of x under the action of S_n respectively.

We choose the following set of symmetric generators $S := \{\tau_{1,n}, \dots, \tau_{n-1,n}\}$ of S_n . We claim that with respect to these generators S_n is efficiently represented on the N -qubit space. Indeed, first,

$$\log |S_n| = \log n! < \log n^n = n \log n < \frac{1}{2} \sqrt{2N} \log(2N).$$

Second, we consider the number of elementary unitary gates to generate $P(\tau_{p,q})$, for $p \neq q \in [n]$. Denote by $\{p, q\}$ -qubit the qubit corresponding to the edge $\{p, q\}$. Then the action of σ on edges \mathcal{E}_n is equivalent to the following $(n-2)$ commuting transposition on $\binom{n}{2}$ qubits. Namely let $k \in [n] \setminus \{p, q\}$. Then the action of $\tau_{p,q}$ on \mathcal{E}_n is equivalent to the transposition of the edges $\{k, p\} \leftrightarrow \{k, q\}$ for $k \in [n] \setminus \{p, q\}$. Assume that the edges are arranged lexicographically from right to left:

$$\{n-1, n\}, \{n-2, n\}, \{n-2, n-1\} \dots, \{2, 3\}, \{1, n\}, \dots, \{1, 2\}. \quad (4.2)$$

Suppose that we use only the transposition between the two neighboring edges in the above ordering to achieve the transposition $\{k, p\} \leftrightarrow \{k, q\}$. Then we need less than $n(n-1)$ neighboring transpositions. Hence the action of any transposition $\tau \in S_n$ on $\binom{n}{2}$ qubits can be implemented with less than $3! \binom{n}{3}$ neighboring transposition on $\binom{n}{2}$ qubits. Equivalently, the unitary transformation $P(\tau)$ on the space $\otimes^{\binom{n}{2}} \mathbb{C}^2$ can be implemented with less than $3! \binom{n}{3}$ swaps of neighboring qubits.

Third, recall that for this set of generators S the second eigenvalue λ_2 of the Laplacian is 1 [8]. Hence the action of S_n on $\binom{n}{2}$ qubit space is efficiently represented.

Define $Q_N := Q(\frac{1}{n}\mathbf{1}_{\{id\} \cup S})$. Fix x . Note that $|y\rangle$ is an eigenvector of $\rho(x)$ and of $Q_N^l(|x\rangle\langle x|)$. Observe next that if $y \notin \text{orb}(x)$ then $\rho(x)|y\rangle = Q_N^l(|x\rangle\langle x|)|y\rangle = 0$. Hence $\lambda_y = \langle y|\rho(x)|y\rangle = \langle y|Q_N^l(|x\rangle\langle x|)|y\rangle = 0$. Otherwise $|y\rangle$ is an eigenvector of $Q_N^l(|x\rangle\langle x|)$ corresponding to the eigenvalue $\langle y|Q_N^l(|x\rangle\langle x|)|y\rangle = \text{tr } Q_N^l(|x\rangle\langle x|)(|y\rangle\langle y|)$. The arguments of the proof of Lemma 4 yield

$$|\langle y|(\rho(x) - Q_N^l(|x\rangle\langle x|))|y\rangle| \leq \sqrt{H(x)}e^{-\frac{l}{n}} \leq \sqrt{n!}e^{-\frac{l}{n}}. \quad (4.3)$$

Hence, the GIP boils down to the problem how good we can estimate $\text{tr } Q_N^l(|x\rangle\langle x|)(|y\rangle\langle y|)$. Indeed, observe:

$$\lambda_y = \langle y|\rho(x)|y\rangle = \langle x|\rho(x)|x\rangle = \frac{|H(x)|}{n!} \geq \frac{1}{n!}, \quad \text{for } y \in \text{orb}(x). \quad (4.4)$$

Letting $l = n^3$ in (4.3) we obtain that λ_y is well approximated by $\text{tr } Q_N^l(|x\rangle\langle x|)(|y\rangle\langle y|)$. Suppose that $G(x)$ is rigid, i.e., $|H(x)| = 1$. Then using the estimate of λ_y explained in §3 one needs to distinguish two Bernoulli processes with $p = \frac{n^3+1}{2n!}$, (if $y \in \text{orb}(x)$), and $p = \frac{1}{2}$, (if $y \notin \text{orb}(x)$). This will not be possible by repeating a polynomial time of measurement discussed in §3.

However, if we assume Hypothesis 1 then we can find out if in polynomial time if $n! \text{tr } Q_N^{n^3}(|x\rangle\langle x|)(|y\rangle\langle y|)$ is zero or positive integer. In the second case this means that $y \in \text{orb}(x)$ and the closest integer to $n! \text{tr } Q_N^{n^3}(|x\rangle\langle x|)(|y\rangle\langle y|)$ is $|H(x)|$. In particular, if $y = x$ we can determine $|H(x)|$.

Similar arguments apply to \mathcal{G} , which is a subgroup of permutation matrices in $U(2^N)$ and efficiently represented.

Acknowledgment I thank Karol Życzkowski for his help in preparing this paper.

References

- [1] D. Aharonov and A. Ta-Shma, Adiabatic Quantum State Generation and Statistical Zero Knowledge, *STOC* 2003, 20–29.
- [2] L. Babai, D.Yu. Grigoryev and D.M. Mount, Isomorphism of graphs with bounded eigenvalue multiplicity, *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, 1982, pp. 310–324.
- [3] R. Beals. Quantum computation of Fourier transforms over symmetric groups, *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 4853, 1997.
- [4] H. Bodlaender, Polynomial algorithms for graphs isomorphism and chromatic index on partial k -trees, *J. Algorithms* 11 (1990), 631–643.
- [5] A.K. Ekert, C.M. Alves, D.K. L. Oi, M. Horodecki, P. Horodecki and L.C. Kwek, Direct estimations of linear and nonlinear functionals of a quantum state, *Phys. Rev. Lett.* 88 (2002), 215501.
- [6] M. Ettinger and Peter Hoyer, A quantum observable for the graph isomorphism problem, arXiv:quant-ph/9901029.

- [7] I.S. Filotti and J.N. Mayer, A polynomial-time algorithm for determining the isomorphism of graphs of fixed genus, *Proceedings of the 12th Annual ACM Symposium on Theory of Computing*, 1980, pp.236-243.
- [8] L. Flatto, A.M. Odlyzko, and D.B. Wales, Random shuffles and group representations, *Annals of Probability*, 13 (1985), 154–178.
- [9] M.R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman, 1979.
- [10] S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen, Limitations of quantum coset states for graph isomorphism, *Journal of the ACM* 57 (2010), no. 6, article 34, Proceedings 38th ACM Symposium on Theory of Computing (STOC’06), pp. 604-617, 2006
- [11] R.A. Horn and C.R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, 1991.
- [12] R. Jozsa, Quantum factoring, discrete logarithms and the hidden subgroup problem, *Computing in Science & Engineering* 3 (2001), 34–43, arXiv:quant-ph/0012084.
- [13] J. Kabler, U. Schaninger and J. Toran, *The Graph Isomorphism Problem: Its Structural Complexity*, Birkhauser, 1993.
- [14] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walks, *London Math. Soc. Lecture Note Ser.*, 218, Cambridge Univ. Press, 1995, 155–189.
- [15] E.M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Computer & System Sciences*, 25 (1982), 42–65.
- [16] G. Miller, (1980), Isomorphism testing for graphs of bounded genus, *Proceedings of the 12th Annual ACM Symposium on Theory of Computing*, 1980, pp. 225-235.
- [17] J. A. Miszczak, Z. Puchała, P. Horodecki, A. Uhlmann, K. Życzkowski, Sub- and super-fidelity as bounds for quantum fidelity, *Quantum Information and Computation*, 9 (2009), 0103-0130.
- [18] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- [19] C. Moore, A. Russell and L.J. Schulman, The Symmetric Group Defies Strong Fourier Sampling, *SIAM J. Computing* 37 (2008) 1842–1864, 2008, Proc. 46th FOCS 479-488, 2005, arXiv:quant-ph/0501056.
- [20] J. Watrous. Succinct quantum proofs for properties of finite groups, *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, pages 537-546, 2000.
- [21] J. Watrous, Quantum algorithms for solvable groups, *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 60 - 67, 2001, arXiv:quant-ph/0011023.